Certificate Trust Lists

What Are They?

Why Are They Useful?

Trevor Freeman
Program Manager
Microsoft Corporation

Where Did CTL's Come From?

- Microsoft development.
- Original targeted for cross certification without directory dependency
  - Now depreciated in in favor of "son of 2459"

What's in a CTL?

- Its signed data content
  - Currently PKCS7
  - Would also work with CMS
- Policy information
  - Set of OID's
- Validity period
- List of trusted certificates as hashes
- Set of extensions

CTL ASN.1 Structure

```
CertificateTrustList ::= SEQUENCE
    version                 Version DEFAULT v1,
    subjectUsage            Subject Usage,
    listIdentifier          ListIdentifier          OPTIONAL,
    sequenceNumber          INTEGER                 OPTIONAL,
    thisUpdate              ChoiceOfTime,
    nextUpdate              ChoiceOfTime
    subjectAlgorithm        AlgorithmIdentifier,
    trustedSubjects         TrustedSubjects
    extensions              Extensions              OPTIONAL
```

New ASN.1 Content

- SubjectUsage –
  - Sequence of 1 or more policy OIDs
    - Same structure as EKU
- ListIdentifier
  - Octet string
- TrustedSubjects
  - Hash of certificate (octet sting)
  - Sequence of attribute type & value pairs (optional)

What Do CTLs Do?

- Express policy regarding a set of hashes
  - Currently certificates
  - Could apply to other sets of hashes.
- Leave the original certificate intact
- Provide delivery vehicle for certificates and policy
- Push or pull distribution

Why Would You Want to Do This?

- Root certificate distribution
  - Original hierarchy remains intact
  - No dependency on client enrolment
  - No need for client UI
- Certificate distrust list
- Compromised key list
- Bad timestamp or notary list

Usage Scenario 1

- Consumers on the internet
  - Remove dependency on Browser update for Trust update
  - Prevent pointless UI to consumer
  - Lower cost of entry for new comersial Cas
  - No dependency on client enrolment
  - Single CTL could work with multiple venders products

Usage Scenario 2

- Enterprise PKI applications without dependency on enrolment
  - Venders could sign CRL for new Enterprise root
    - Different policy to commercial CA’s
  - Don't need a cert to participate in PKI applications
    - TLS server authentication
    - S\MIME signature verification

Way Forward

- Microsoft turn over CTL to IETF
  - Royalty free patent license
  - Author I-D with any interested parties
  - IETF would henceforth own CTLs
  - Microsoft would revise current implementation to meet new RFC requirements

Questions